FIREEYE™

LIVRE BLANC

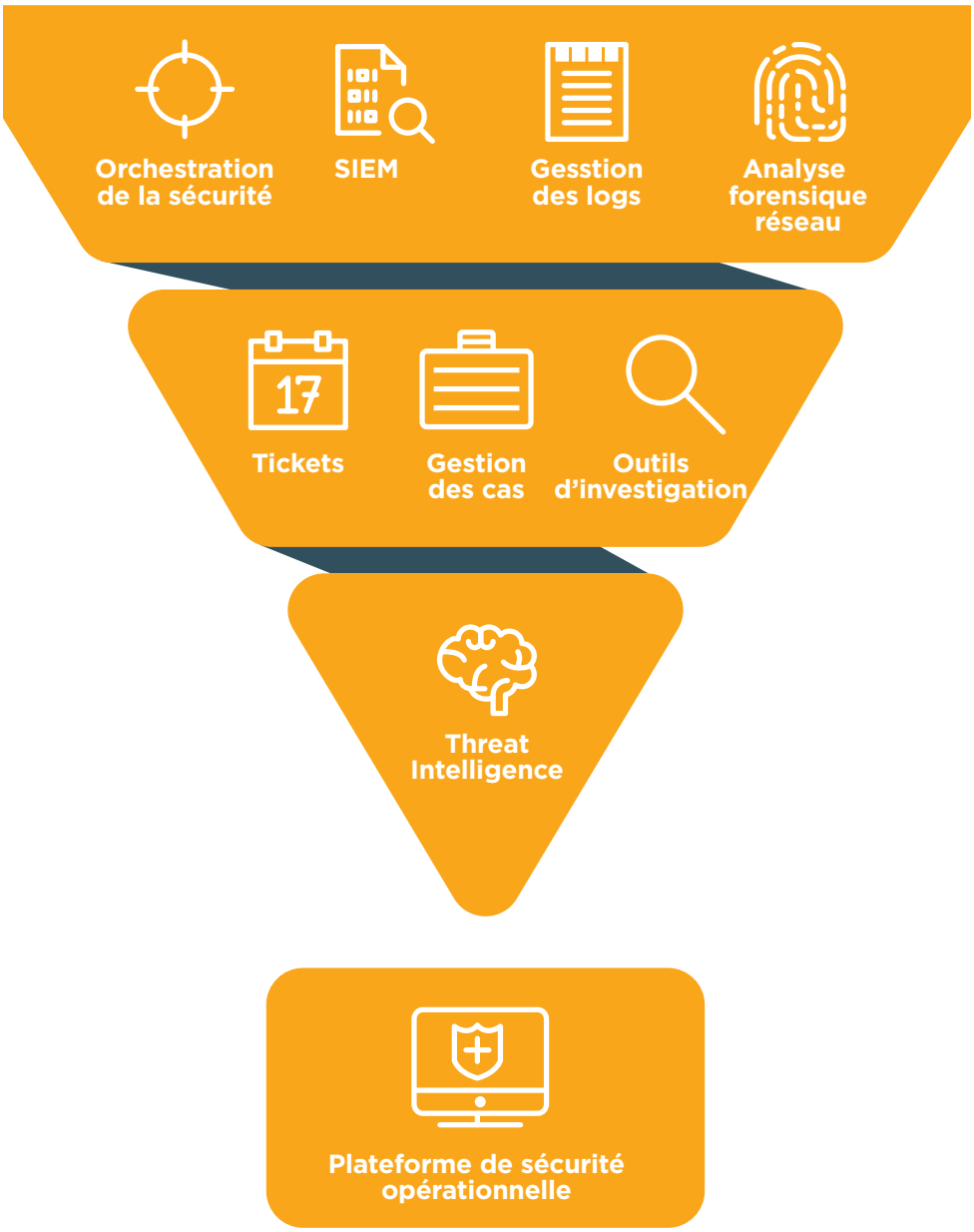
Prenez le contrôle de votre sécurité

Vers une protection unifiée et simplifiée pour toutes les entreprises

Nouvelle approche de la sécurité opérationnelle

Dans un monde où presque chaque jour apporte son lot de nouvelles menaces, de nombreuses entreprises choisissent de consacrer davantage d'efforts et de moyens au renforcement de leur sécurité. Et elles ont raison. Leur raisonnement est simple : si une entreprise – quelle que soit sa taille – possède ce que les cybercriminels recherchent (informations, argent, forte exposition à d'éventuelles nuisances, etc.), elle en deviendra tôt ou tard la cible. Seulement voilà, la mise sur pied d'un écosystème de sécurité efficace représente un fardeau énorme pour des entreprises aux ressources limitées. Confrontées aux mêmes risques que les géants internationaux, elles disposent cependant d'une fraction de leurs moyens humains et financiers.

Hormis la question purement financière, l'achat d'un nouvel équipement ou la souscription d'un nouveau service produisent rarement les effets escomptés. S'il ne s'accompagne pas de mesures de sécurité adaptées, l'ajout de produits spécialisés augmente en effet la complexité, la masse salariale, les tâches manuelles sujettes aux erreurs et, potentiellement, le risque. Étonnamment, les produits les plus récents mettent du temps à répondre à ces besoins pressants et bien connus des clients.



La bonne nouvelle, c'est qu'une approche plus holistique de la cybersécurité est actuellement en train d'émerger.

Plateformes de sécurité
En agissant comme la cellule de commande de votre centre opérationnel de sécurité (SOC), les plateformes de sécurité constituent une réponse innovante aux problématiques opérationnelles actuelles. Conçues pour intégrer et automatiser vos opérations de sécurité, elles permettent à vos équipes de bloquer les menaces plus rapidement, tout en réduisant vos coûts opérationnels. Mais attention : toutes les plateformes ne se valent pas.

Par exemple, certaines solutions de gestion des événements et des informations de sécurité (SIEM) tentent de se repositionner comme consoles de sécurité opérationnelle, avec des avantages tactiques pourtant très limités. Elles se contentent en effet d'agréger des volumes d'alertes sans automatisation ni analyses contextuelles, ce qui génère davantage de problèmes que de solutions pour les analystes du SOC.

C'est pourquoi ce livre blanc vous invite à faire le point sur les fonctionnalités essentielles d'une plateforme de sécurité, mais aussi à dresser l'inventaire des facteurs de sélection d'un fournisseur dans ce domaine. Aucune innovation ne dispense les RSSI de mettre en place des technologies, processus et compétences de pointe. Les plateformes de sécurité ont pour vocation d'unifier la gestion de la sécurité opérationnelle des entreprises. En ce sens, elles présagent d'une simplification, de gains d'efficacité et, au final, d'une sécurité renforcée de leurs réseaux informatiques.

Visibilité

La visibilité désigne la capacité d'une entreprise à détecter, évaluer et alerter sur l'impact des attaques. Tout l'enjeu consiste à identifier les menaces qui planent sur elle et à distinguer celles qui représentent un réel danger. Qui dit sécurité dit visibilité. De fait, tout angle mort dans votre infrastructure pourra entraîner de graves problèmes.

À mesure que les cybermenaces évoluent, de nouvelles zones d'ombre sont susceptibles d'apparaître sur votre réseau. Par exemple, les entreprises d'aujourd'hui cherchent à gagner en visibilité sur les points de connexion de leurs fournisseurs, de leurs filiales et d'autres interconnexions inexistantes par le passé.

L'utilisation de plus en plus répandue du cloud apporte également son lot de vulnérabilités et d'angles morts. Stocker des informations confidentielles et exécuter des opérations critiques dans le cloud peut créer un vrai casse-tête en termes de sécurité, dans la mesure où les configurations et la gestion des identifiants sont difficiles à centraliser.

Pour améliorer le degré de visibilité, une plateforme de sécurité opérationnelle doit identifier rapidement les intrusions, repérer les vulnérabilités de manière proactive et centraliser/synthétiser les données de sécurité pour anticiper les actions des attaquants.

Identification rapide des violations de sécurité
Sur le front de la sécurité, les entreprises cherchent évidemment à jouer la carte de la prévention. Toutefois, face à des cybercriminels de plus en plus habiles dans l'art de manipuler les faiblesses humaines et technologiques, les attaques finissent tôt ou tard par aboutir. Reste alors à savoir combien de temps les attaquants pourront évoluer sans se faire repérer. Dans le monde entier, le délai médian entre une compromission et sa détection (durée d'implantation) reste de 99 jours, ce qui laisse largement le temps aux attaquants de faire main basse sur des informations sensibles, voire d'effacer leurs traces.[1]

En conséquence, une plateforme de sécurité doit compléter ses mesures préventives par des moyens de détection rapide. L'objectif : identifier le malware utilisé, évaluer rapidement les dégâts et le niveau d'exposition, et intégrer ces analyses à la fonction globale de sécurité opérationnelle. Dans un monde où chaque minute d'infiltration des hackers sur un réseau se compte en centaines, voire en milliers d'euros, une plateforme de sécurité opérationnelle doit pouvoir détecter une violation de données non plus en heures ou en jours, mais en quelques minutes seulement.

Interprétation et décryptage des alertes
Un autre enjeu majeur consiste à identifier les menaces réelles dans la masse de faux positifs. En effet, parmi les 17 000 alertes brutes hebdomadaires que reçoit une entreprise, seules 19 % sont considérées comme fiables et 4 % donnent lieu à une investigation. Le problème de cette surabondance d'alertes ne se limite pas aux interférences qu'elle créé : elle a aussi un coût.
En moyenne, le temps qu'une entreprise passe à traiter des informations inexactes et erronées peut lui faire perdre 1,27 million de dollars par an.[2]

Sans le contexte nécessaire, les décisions des analystes en sécurité relèvent davantage de la gageure. C'est pourquoi une plateforme de sécurité efficace doit extraire et analyser les menaces, puis automatiser la validation des alertes afin d'éliminer les faux positifs. Elle doit également permettre aux équipes de sécurité de tailler dans la masse d'alertes pour cibler directement les menaces les plus dangereuses.

Lecture et anticipation des comportements des attaquants
Ces dernières années, l'efficacité des solutions de détection traditionnelles basées sur les signatures a sérieusement baissé. En cause : la capacité des attaquants à réécrire leur code pour échapper à toute détection, mais aussi une évolution progressive vers le vol d'identifiants et d'autres techniques hors malware.[3]

Pour être efficace, une plateforme de sécurité opérationnelle doit donc pouvoir identifier une menace qu'elle n'a jamais vue auparavant. Elle doit s'appuyer sur une analytique avancée pour modéliser les comportements des attaquants et anticiper leurs prochains mouvements. Une telle codification des comportements passe par l'alliance de l'analytique, de la Threat Intelligence et d'une expérience pratique acquise sur le terrain. C'est pourquoi une bonne solution ne se basera pas uniquement sur

1 FireEye (2017). « M-Trends 2017: A View from the Front Lines ».
2 Ponemon Institute (janvier 2015). « The Cost of Malware Containment ».
3 Joshua Goldfarb (26 octobre 2016). « 20 Endpoint Security Questions You Never Thought to Ask ».

le machine learning ou les analyses comportementales. Elle devra également aider les analystes à prioriser les menaces, les isoler et adopter les bons réflexes pour les neutraliser.

Réponse

Au vu du battage médiatique actuel autour des cyber-attaques, nul besoin de travailler dans le secteur de la sécurité pour savoir que les réponses à incident s'avèrent tout aussi importantes que leur prévention. Un processus efficace passe par des alertes fiables, une file d'attente triée par ordre de priorité, des analyses précises et une gestion fluide des incidents. Au premier abord, le workflow en tant que tel ne semble pas primordial pour une entreprise lambda. Toutefois, les chiffres prouvent le contraire. Ainsi, l'année dernière, il a fallu en moyenne 82 jours aux entreprises pour circonscrire et neutraliser une attaque avancée.[4]

Pour réduire ce délai, une plateforme de sécurité opérationnelle doit donc intégrer toutes les opérations de sécurité, fonder ses réponses sur des informations fiables, fournir des capacités de gestion des dossiers et améliorer l'efficacité des équipes.

Intégration des opérations de sécurité

Une plateforme de qualité permet aux équipes de sécurité de passer plus rapidement des alertes à la neutralisation. Toutefois, les délais de réponse dépendent généralement de la vitesse d'interprétation des alertes. Si vos alertes proviennent de multiples sources et sont fournies en l'état, sans contexte ni corrélation, vous ne serez pas beaucoup plus avancé. Une plateforme efficace combine les logs, puis opère des rapprochements avec les analyses et informations de veille pour faire émerger de nouvelles menaces. Ainsi, elle s'avère bien plus puissante que la somme de ses composants.

La Threat Intelligence au service d'une réponse plus ciblée

La fiabilité et la fidélité des informations sont deux des piliers essentiels d'une plateforme de sécurité mature. Toutefois, pour remplir leur mission, ces informations doivent pouvoir être appliquées directement à l'environnement opérationnel. En d'autres termes, si l'information ne peut se traduire rapidement en mesures de protection concrètes, elle ne servira pas à grand-chose. C'est pourquoi les plateformes de sécurité devraient toujours fournir une Threat Intelligence contextualisée et en prise avec les réalités de l'entreprise et de l'attaque en question. Dans l'idéal, cette information devrait être disponible à la demande pour faciliter les investigations.

Gestion des incidents

La détection repose souvent sur des membres individuels de l'équipe SOC. Quant à l'investigation et l'orchestration, elles s'appuient sur plusieurs intervenants qui doivent accomplir les tâches qui leur incombent, créer des rapports et partager des informations sensibles. Malheureusement pour les équipes SOC, les outils traditionnels de communication et de gestion de projets sont loin de répondre aux besoins de coordination de ces activités. Une plateforme de sécurité doit donc fournir aux équipes des outils simples pour l'assignation et le suivi des tâches, la gestion de leur file d'attente et le partage de connaissances en vue d'une résolution efficace.

Efficacité renforcée des équipes

À mesure que les menaces évoluent, les entreprises se livrent une bataille acharnée pour attirer les meilleurs talents de la cybersécurité, dans un contexte de pénurie de candidats. Aux États-Unis, plus de 209 000 postes de cybersécurité restent vacants, tandis que les offres d'emploi dans ce secteur ont augmenté de 74 % ces cinq dernières années.[5] Et même avec la meilleure volonté du monde, la mise en place d'une sécurité opérationnelle 24h/7j se heurte souvent à des réalités budgétaires qui ne permettent pas de la doter en effectifs adéquats. Compte tenu du manque de ressources dans la plupart des entreprises, assigner les analystes au traitement d'alertes issues de systèmes de sécurité conventionnels revient à perdre du temps et de l'argent. Ces processus manuels s'avèrent aussi inefficaces que sujets aux erreurs. En somme, toute plateforme de sécurité incapable d'automatiser ce type de tâches répétitives et chronophages affaiblit le niveau de sécurité de l'entreprise et démotive ses salariés.

Coût total de possession

Dans le secteur de la cybersécurité, le coût total de possession (TCO) fait partie des thématiques récurrentes auxquelles personne n'échappe. Les entreprises aiment comparer les produits en fonction de leur prix d'achat. En principe, cela ne pose aucun problème. Seulement voilà, les produits en question s'avèrent souvent très différents. Il faut aussi garder à l'esprit que chaque euro consacré à la cybersécurité est un euro qui ne sera pas investi dans la stratégie de croissance de l'entreprise. Si bien que les priorités doivent être évaluées en conséquence.

Puisque la protection du capital stratégique de l'entreprise est appelée à rester un poste essentiel du budget d'exploitation, il convient d'élargir le concept de TCO pour élever le débat de la cybersécurité à un rang plus stratégique. Cette approche permet d'adopter une vue plus complète sur les coûts et les avantages des plateformes de sécurité.

Coûts financiers

Matériels et logiciels, contrats de licence et mises à niveau, déploiement et maintenance… tous ces postes de coûts font généralement l'objet d'une attention toute particulière des décideurs. Bien que simples en apparence, ils cachent souvent des problèmes de redondance et d'inefficacité de l'infrastructure, à commencer par l'existence de plusieurs solutions aux mêmes fonctionnalités, ou encore la présence de produits spécialisés et mal intégrés qui requièrent une maintenance excessive, des mises à niveau fréquentes et, au final, des interruptions de service plus longues.

Une plateforme de sécurité efficace associe un large éventail de fonctionnalités, y compris la protection du réseau, des e-mails et des terminaux ; un système SIEM et d'orchestration ; et des capacités forensiques et de gestion des logs. Pour contribuer à la rationalisation des coûts, elle doit soit proposer d'intégrer le patchwork de produits existants, soit permettre de s'en débarrasser.

4 Ponemon Institute (mars 2016). « The State of Malware Detection and Prevention ».
5 Ariha Setalvad (31 mars 2015). « Demand to fill cybersecurity jobs booming ».

Coûts d'exploitation

Les dépenses des entreprises ne se limitent pas au simple achat d'équipements et à la souscription de services. Les coûts d'exploitation couvrent également le temps et les moyens consacrés au recrutement et à l'embauche de talents rares, à leur formation sur vos produits, ou encore au pilotage des opérations courantes. Dans la plupart des entreprises, ces dépenses s'avèrent aussi inévitables que les coûts financiers directs.

Ainsi, les entreprises devraient répartir leur temps avec soin, car ce temps est inévitablement de l'argent. Lors de l'évaluation des plateformes de sécurité, elles doivent donc se focaliser sur un certain nombre de critères :

- Produits aux fonctionnalités plus larges pour la réduction, voire l'élimination des coûts et du temps consacrés à la formation des équipes sur un patchwork de solutions non intégrées
- Fonctions de détection avancées pour éviter les phénomènes d'accoutumance aux alertes et détecter rapidement les menaces réelles
- Fonctionnalités d'orchestration et d'investigation renforcées pour recentrer le travail des équipes sur les tâches les plus créatrices de valeur

L'automatisation réduit les processus manuels répétitifs comme la validation des alertes. Trop souvent, les professionnels de la sécurité passent 80 % de leur temps à accomplir ces tâches, ce qui génère chez eux un sentiment de lassitude qui les pousse au départ. En automatisant ces activités, une plateforme de sécurité opérationnelle leur permet de se concentrer sur des tâches à plus forte valeur stratégique, comme la recherche et la prévention des menaces et, en cas de violation avérée, la réponse et la neutralisation de l'incident.

Pour atténuer les effets des inévitables départs de collaborateurs, une bonne plateforme de sécurité devra codifier et automatiser les activités de l'équipe de sécurité pour que les bonnes pratiques soient ancrées à la structure de l'entreprise, et non tributaires de tel ou tel individu.

Enfin, la continuité de service influence grandement les coûts d'exploitation. En d'autres termes, fidéliser des professionnels de la sécurité s'avère tout aussi difficile que de les recruter. À la différence près que les embauches peuvent se planifier, pas les départs. Or, lorsqu'un talent décide de partir, son absence risque de créer un vide nuisible à la sécurité de l'entreprise. C'est pourquoi une plateforme de sécurité opérationnelle efficace devra confier aux équipes les outils, tâches et connaissances adaptés à leur profil de compétences afin de minimiser le turnover.

Tableau 1. Plateforme de sécurité : checklist des fonctionnalités critiques

Hausse de la visibilité	
Détection des intrusions en quelques minutes	✓
Fusion et priorisation des alertes les plus critiques	✓
Anticipation des comportements des attaquants	✓
Accélération des réponses	
Console centralisée pour toute l'infrastructure	✓
Réponses assistées par des informations de Threat Intelligence	✓
Gestion des incidents	✓
Optimisation des coûts	
Rationalisation des investissements financiers	✓
Amélioration de l'efficacité des équipes	✓
Continuité de service	✓

Conclusion

Pour de nombreuses entreprises, les plateformes de sécurité opérationnelle offrent une mine d'avantages. Bien entendu, comme pour toute décision d'achat, il est important d'exiger des fournisseurs une proposition et des engagements clairs afin de bien cerner les capacités concrètes des solutions proposées. C'est là le seul moyen de garantir des niveaux de sécurité élevés à toutes les entreprises, y compris celles aux budgets les plus contraints.

Pour en savoir plus, rendez-vous sur **www.fireeye.fr**

FireEye, France | Nextdoor Cœur Défense
110 Esplanade du Général de Gaulle
92931 Paris La Défense Cedex 92974
+33 1 70 61 27 26
france@FireEye.com | www.FireEye.fr
601 McCarthy Blvd. Milpitas, CA 95035 |
+1 408 321 6300 | info@FireEye.com

À propos de FireEye, Inc.

FireEye est spécialisé dans la cybersécurité axée sur la Cyber Threat Intelligence (CTI). Prolongement naturel et évolutif des opérations de sécurité des clients, la plateforme unique de FireEye combine des technologies de sécurité innovantes, des services de CTI d'envergure internationale et les services réputés de Mandiant® Consulting. FireEye simplifie ainsi la cybersécurité et son administration, devenant un allié précieux des entreprises confrontées au casse-tête que représentent la prévention et la neutralisation des cyberattaques.

FIREEYE